CS402 - Project 1

Yen Nguyen, Long Pham, Daniel Ziabicki

February 9th, 2026

Part 1: Trace AES

(1) State After Round 4

The state after round 4 is: `2574ffe6feac57434aee990f74001f11`

(2) Flipping Bit 12

State Values Per Round

Round	State (original)	State (after flipping)
0	`826a820f7298cdda683e60842c91d593`	`8262820f7298cdda683e60842c91d593`
1	`7be6066fe7280010d02025cb954f2a0c`	`7be6066fe7280010d02025cb760482a4`
2	`100dee3cace2e3804499a3f2a4af5635`	`a7ba2c495ae31476de75d58480bd4403`
3	`6ccb3d38964808dc12e09a1d27c2cd6c`	`3fa21cd827b470cfb7fe29bc6cf0c684`
4	`2574ffe6feac57434aee990f74001f11`	`07dc2e55c739e938dd1d29a598b43c73`

Bit Differences Per Round

Round	Bits Different
0	1
1	15
2	69
3	60
4	67

(3) Discussion

When we flipped just one bit of the plaintext, we saw that the state values after each round changed drastically compared to the original encryption. This demonstrates one of the key properties of a strong block cipher: even a small change in the input produces outputs that appear completely unrelated to the original (avalanche effect), making the ciphertext look essentially random to anyone without the key. In other words, AES behaves like a pseudorandom permutation and its outputs are indistinguishable from a perfect cipher if you don't know the key.